KSIĘGA PROCEDUR
Z ZAKRESU
OCHRONY DANYCH OSOBOWYCH

Śląskiego Funduszu Rozwoju Sp. z o.o.
w Katowicach

Wersja 2		**Pieczęć firmowa:**	
Opracował:	**Data:**	**Zatwierdził:**	**Data:**
Anna Mianowska			.

Spis treści

§ 1 POSTANOWIENIA OGÓLNE

1. Księga procedur z zakresu ochrony danych osobowych podmiotu (zwana dalej: Księgą procedur ODO) określa zasady dotyczące przetwarzania danych osobowych w Spółce i została opracowana na podstawie *Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE* (ogólne rozporządzenie o ochronie danych) (zwane dalej: RODO).

2. Księga procedur ODO została przyjęta Uchwałą/Zarządzeniem nr ...../2025 z dnia .....2025 roku, z datą obowiązywania od .....2025 roku.

§ 2 SŁOWNIK POJĘĆ

Ilekroć w Księdze procedur ODO jest mowa o:

1. **Spółka—** należy przez to rozumieć Śląski Fundusz Rozwoju Sp. z o.o. w Katowicach dalej ŚFR.

2. **ADO** - należy przez to rozumieć Administratora Danych Osobowych, którym jest Spółka. W imieniu ADO może występować Prezes Spółki/Członek Zarządu odpowiedzialny za ochronę danych osobowych w Spółce.

3. **IOD** - należy przez to rozumieć Inspektora Ochrony Danych, powołanego na podstawie odrębnego zarządzenia/uchwały.

4. **Pracowniku** - należy przez to rozumieć osobę zatrudnioną w Spółce na podstawie umowy o pracę /kontraktu menadżerskiego/ umowy cywilnoprawnej, a także osoby przyjęte na staż czy praktykę, a także pracowników oddelegowanych do pracy w Spółce na podstawie odrębnych umów.

5. **Zakładzie pracy** – należy przez to rozumieć Śląski Fundusz Rozwoju Sp. z o.o. w Katowicach.

6. **Nośnikach danych** – należy przez to rozumieć przedmiot fizyczny, na którym możliwe jest zapisanie informacji i późniejsze ich odczytanie. Dzielimy je na:

    a. nośniki magnetyczne np.: dyski zewnętrzne;

    b. nośniki optyczne np.: kartka papieru, pendrive, płyty CD, płyty DVD.

§ 3 PROCEDURY, WZORY I INSTRUKCJE

1. PROCEDURA ROZPOCZYNANIA ORAZ KOŃCZENIA PRACY W SYSTEMIE

1) Celem procedury jest zabezpieczenie danych osobowych przed nieuprawnionym dostępem i utratą poufności w sytuacji, gdy użytkownik rozpoczyna, przerywa lub kończy pracę w systemie informatycznym przetwarzającym dane osobowe.

2) Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.

3) Użytkownik jest zobowiązany do powiadomienia ADO oraz IOD o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.

4) W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym ADO lub osobę upoważnioną przez ADO, która odpowiada za odblokowanie systemu użytkownikowi.

5) Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. klientom, kontrahentom) wglądu do danych wyświetlanych na monitorach komputerowych – tzw. **Polityka czystego ekranu.**

6) Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu. Jeżeli tego nie uczyni – po upływie 5 minut system automatycznie aktywuje wygaszacz.

7) Po zakończeniu pracy, użytkownik zobowiązany jest:

   a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy

   b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

2. PROCEDURA UDZIELANIA INFORMACJI O NIEOBECNOŚCI WSPÓŁPRACOWNIKÓW

1) Jedyną informacją, jaką można udzielić w przypadku pytań o nieobecność współpracownika to – „TAK, JEST NIEOBECNY".

2) **Nie wolno udzielać informacji o przyczynie nieobecności** współpracownika. WYJĄTEK stanowi w tym przypadku przełożony.

3. PROCEDURA NADAWANIA UPRAWNIEŃ DO PRZETWARZANIA DANYCH OSOBOWYCH

1) Na zlecenie ADO lub osoby przez niego upoważnionej następuje przyznanie lub anulowanie upoważnienia pracownikowi do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze papierowym.

2) Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielony innej osobie.

3) Przed przyjęciem do pracy Prezes Spółki/Członek Zarządu/pracownik odpowiedzialny za sprawy personalne powiadamia IOD o przyjęciu nowego pracownika i ustala termin szkolenia z zakresu bezpieczeństwa informacji, w tym ochrony danych osobowych.

4) IOD ustala z przełożonym nowo zatrudnionego pracownika zakres uprawnień oraz poziom dostępu do danych, który wynika z przydzielonego zakresu czynności.

5) Przed nadaniem upoważnienia do przetwarzania danych:

   a) IOD szkoli daną osobę z zakresu bezpieczeństwa informacji, w tym ochrony danych osobowych,

   b) pracownik podpisuje oświadczenie o zachowaniu poufności, którego wzór stanowi

Załącznik nr 1 do niniejszej Procedury.

c) IOD przekazuje zakres uprawnień i poziom dostępu do danych osobom odpowiedzialnym za administrowanie systemami informatycznymi (HelpDesk, ABI Informatics),

d) przygotowane upoważnienie IOD przekazuje do akceptacji ADO

6) ADO jest zobowiązany do aktualizacji upoważnień, jak również ich zakresów.

7) IOD jest zobowiązany prowadzić *Rejestr upoważnień* (*Załącznik nr 2* do niniejszej Procedury).

Załącznik nr 1** do Procedury nadawania uprawnień do przetwarzania danych – **WZÓR OŚWIADCZENIA O ZACHOWANIU POUFNOŚCI

.....

miejscowość, data

.....

imię i nazwisko

.....

stanowisko

Oświadczenie o zachowaniu poufności

Oświadczam, iż zostałam/em zapoznana/ny z przepisami dotyczącymi ochrony danych osobowych oraz wprowadzonymi i wdrożonymi do stosowania przez Administratora procedurami związanymi z ochroną danych osobowych i bezpieczeństwem informacji.

Zobowiązuję się do:

1. zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań służbowych lub obowiązków służbowych,

2. niewykorzystywania danych osobowych w celach pozasłużbowych, o ile nie są one jawne,

3. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych, o ile nie są one jawne,

4. korzystania z wyposażenia IT oraz oprogramowania wyłącznie w związku z wykonywaniem obowiązków służbowych,

5. wykorzystywania jedynie legalnego oprogramowania pochodzącego od Pracodawcy/ Zleceniodawcy*,

6. należytej dbałości o wyposażenie IT i oprogramowanie.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane przez Pracodawcę/ Zleceniodawcę* odpowiednio:

a) za ciężkie naruszenie obowiązków służbowych w rozumieniu art. 52 § 1 pkt 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy;

b) ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;

c) ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny;

d) Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

.....

podpis

* *niepotrzebne skreślić*

Załącznik nr 2 *do Procedury nadawania uprawnień do przetwarzania danych –* ***WZÓR REJESTRU UPOWAŻNIEŃ.***

REJESTR UPOWAŻNIEŃ – WZÓR

Nr upoważnienia	Imię i nazwisko pracownika	Zbiór			System informatyczny		Okres obowiązywania	
		Zbiór 1	Zbiór 2	Zbiór 3	System 1	System 2	od -	- do
1/2022								
2/2022								

4. METODY I ŚRODKI UWIERZYTELNIANIA

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

1) Ogólne zasady postępowania z hasłami

a) ADO informuje mailem/ustnie użytkownika o nadaniu pierwszego hasła do systemu.

b) Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.

c) Użytkownik systemu w trakcie pracy w aplikacji/systemie powinien cyklicznie zmieniać swoje hasło.

d) Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.

e) Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.

f) Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.

2) Hasła do sieci i serwera

a) Hasło dostępu do (serwera/sieci) składa się z zestawienia kilku słów oraz jak największej ilości małych i dużych liter, cyfr i znaków specjalnych.

b) Zmiana hasła powinna odbywać się raz na 6 miesięcy i może być wymuszana przez system.

3) Hasła do programów przetwarzających dane osobowe

a) Hasło dostępu do programów składa się z zestawienia kilku słów oraz jak największej ilości małych i dużych liter, cyfr i znaków specjalnych.

b) Zmiana hasła powinna odbywać się raz na 30 dni.

4) Hasła administratora

a) Hasło administratora składa się z zestawienia kilku słów oraz jak największej ilości małych i dużych liter, cyfr i znaków specjalnych.

b) Administrator systemu zobowiązany jest zmieniać swoje hasło nie rzadziej niż co 90 dni.

5. PROCEDURA TWORZENIA KOPII ZAPASOWYCH

1) Kopie zapasowe dokumentów z dysków sieciowych, serwerów oraz baz danych tworzone są w sposób regularny i automatyczny. Kopie danych wprowadzanych do poszczególnych systemów wraz z odpowiedzialnością dot. ich utraty oraz zachowaniem poufności, zostały określone w umowach z poszczególnymi podmiotami.

2) Okres przechowywania poszczególnych danych w kopiach bezpieczeństwa określają odrębne przepisy prawa, któremu podlega Spółka.

3) Dostęp do kopii mają upoważnieni do administrowania danymi pracownicy.

4) Informatyk sprawuje nadzór nad poprawnym wykonywaniem i działaniem funkcji kopiowania danych.

5) Przynajmniej raz w roku należy wykonać awaryjne odtworzenie kopii bezpieczeństwa.

6) Wykaz sporządzanych kopii bezpieczeństwa prowadzi Administrator/Informatyk wraz z informacją dot. odtworzenia kopii zapasowych (prawidłowe, nieprawidłowe, czas przywrócenia).

6. PROCEDURA ZABEZPIECZENIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI

1) Nośniki danych należy przechowywać w taki sposób, aby chronić je przed osobami nieupoważnionymi i zagrożeniami naturalnymi.

2) Nie wolno wynosić poza zakład pracy nośników informacji bez zgody ADO.

   a) Nośniki, które są uprawnione do transportu danych poza obszarem ADO powinny posiadać możliwość szyfrowania dysków (laptopy, telefony służbowe, pendrivy, dyski zewnętrzne);

   b) Nośniki, które są uprawnione do użytku na terenie i poza terenem ADO są zarejestrowane w rejestrze nośników;

   c) Rejestr nośników prowadzi ADO lub upoważniony pracownik. Rejestr nośników prowadzony zgodnie ze wzorem - Załącznikiem nr 1 do Procedury nr 15.

3) Pracownicy niezwłocznie i trwale usuwają/kasują dane osobowe z nośników informacji, jeśli nie ma powodu do ich przechowywania lub ustał cel przetwarzania.

4) Uszkodzone lub przestarzałe nośniki informacji, a w szczególności twarde dyski z danymi osobowymi należy niszczyć komisyjnie oraz spisać protokół zniszczenia.

5) W celu zabezpieczenia infrastruktury przed skutkami awarii zasilania zastosowano listwy przepięciowe.

6) Zabezpieczenia jako opis i zastosowanie bezpiecznych i trwałych elementów infrastruktury, wykorzystywanych do przetwarzania danych osobowych:

   a) Komputery służące do przetwarzania danych osobowych są połączone z siecią LAN.

   b) W przypadku, gdy zbiór danych osobowych przetwarzany jest przy użyciu komputera przenośnego, wymagane zabezpieczenia, to: szyfrowanie dysku twardego, szyfrowanie transmisji przy pracy spoza sieci LAN, po zakończeniu pracy przechowywanie w warunkach zapewniających bezpieczeństwo, regularna kopia bezpieczeństwa.

   c) Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają licencje.

7) Zabezpieczenia przed nieuprawnionym dostępem do danych osobowych, w tym środków zapewniających rozliczalność wykonywanych operacji:

   a) Lokalizacja urządzeń komputerowych (komputerów typu PC, skanerów, drukarek) uniemożliwia osobom niepowołanym (np. klientom, kontrahentom) dostęp do nich.

   b) Dostęp do zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej / komputerze przenośnym zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą haseł.

   c) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem loginu oraz hasła.

8) Zabezpieczenia sprzętowych i programowych środków ochrony poufności danych przesyłanych drogą elektroniczną (środków ochrony transmisji);

   a) Zastosowano środki kryptograficzne ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.

9) Zabezpieczenia sprzętowych i programowych środków ochrony przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzanych danych

   a) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.

   b) Użyto system Firewall do ochrony dostępu do sieci komputerowej.

7. PROCEDURA KORZYSTANIA Z SIECI INTERNET ORAZ POCZTY ELEKTRONICZNEJ

1) Pracownik TYLKO do własnej wiadomości zna hasło dostępu do sieci Internet.

2) Pracownik korzysta z sieci Internet wyłącznie w celach służbowych.

3) **Przeglądanie stron internetowych – *PRACOWNIK*:**

   a) nie włącza w przeglądarce autouzupełniania formularzy i zapamiętywania haseł,

   b) NIE MOŻE przeglądać stron internetowych o charakterze przestępczym, hakerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem),

   c) korzysta z szyfrowanego połączenia przez przeglądarkę, o czym świadczą ikonki – kłódka, protokół https,

   d) NIE MOŻE uruchamiać czy zgrywać na dysk twardy komputera nielegalnych programów oraz plików z niewiadomego źródła,

   e) w przypadku wątpliwości co do pochodzenia pliku musi otrzymać każdorazowo zgodę ADO do jego ściągnięcia i uruchomienia,

   f) **ponosi odpowiedzialność za szkody** spowodowane przez oprogramowanie ściągnięte z Internetu i przez niego zainstalowane, co grozi zainfekowaniem sprzętów teleinformatycznych w zakładzie pracy.

4) **Korzystanie z poczty elektronicznej – *PRACOWNIK*:**

   a) nie otwiera podejrzanych e-maili,

   b) nie otwiera linków przesłanych przez nieznanych nadawców,

   c) nie pobiera załączników z nieznanych lub podejrzanych e-maili,

   d) niezwłocznie informuje ADO o niebezpiecznej wiadomości,

   e) szyfruje załączniki zawierające dane osobowe (nadaje hasło, które podaje inną drogą komunikacyjną),

f) zwraca uwagę na poprawność adresu e-mail, na który wysyła wiadomości, **tzw. zasada podwójnej weryfikacji,**

g) dba o wydajność systemu poczty elektronicznej – nie rozsyła wiadomości zawierających załączniki o dużym rozmiarze do wielu adresatów,

h) regularnie kasuje niepotrzebne wiadomości pocztowe zawierające dane osobowe, a pozostałe wiadomości archiwizuje,

i) podczas przesyłania danych osobowych mailem zawiera w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata,

j) nie powinien rozsyłać za pośrednictwem poczty elektronicznej informacji o zagrożeniach dla systemu informatycznego, „łańcuszków szczęścia" itp. Zapisu nie stosuje się wobec osób oddelegowanych do weryfikacji zagrożeń dla systemów informatycznych oraz obsługi incydentów cybernetycznych.

8. PROCEDURA DOTYCZĄCA PUBLIKOWANIA ZDJĘĆ ZAWIERAJĄCYCH WIZERUNEK OSÓB

1) Osoba, której wizerunek ma zostać opublikowany, musi wcześniej wyrazić na to pisemną zgodę.

2) Można odstąpić od zbierania zgód w przypadku, kiedy utrwalanie wizerunku odbywa się z zastosowaniem przepisów ustawy z dnia 4 lutego 1994 r. prawie autorskim i prawach pokrewnych tj. w przypadku rozpowszechniania wizerunku:

   a) osoby powszechnie znanej, jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych;

   b) osoby stanowiącej jedynie szczegół całości takiej jak zgromadzenie, krajobraz, publiczna impreza.

3) Zgoda na udostępnienie wizerunku musi zawierać:

   a) cel przetwarzania danych

   b) informację o czasie publikacji

   c) informację o miejscu opublikowania wizerunku

   d) treść obowiązku informacyjnego

   e) informację o możliwości odwołania w każdym momencie zgody na publikację.

4) Zdjęcie zawierające wizerunek należy usunąć po upływie czasu określonego w zgodzie publikacji.

5) Zdjęcia należy niezwłocznie usunąć również w przypadku, gdy osoba, której dane dotyczą, odwoła zgodę na udostępnianie zdjęć z jej wizerunkiem lub skorzysta z prawa do zapomnienia, ograniczenia przetwarzania lub sprzeciwu.

9. PROCEDURA TRANSPORTOWANIA DOKUMENTÓW

1) ADO wyznacza pracowników mogących transportować dokumenty zawierające dane osobowe.

2) Dokumenty należy przenosić w nieprzezroczystych i trwałych torbach lub teczkach.

3) Dokumenty należy przenosić wyłącznie w celu ich doręczenia.

4) Dokumenty należy transportować najkrótszą drogą do celu.

5) Transportując dokumenty nie należy wchodzić z nimi do sklepów lub do innych zatłoczonych miejsc.

6) W przypadku transportu dokumentów własnym środkiem transportu nie wolno pozostawiać ich w pojeździe bez nadzoru.

7) Od momentu pobrania do momentu dostarczenia dokumentów za ich bezpieczeństwo odpowiada osoba transportująca.

8) Transportowanie dokumentów przez wyznaczone do tego celu firmy kurierskie odbywa się na podstawie zapisów umieszczonych w umowie i w umowie powierzenia oraz na podstawie odrębnych przepisów prawa.

10. PROCEDURA UDZIELANIA INFORMACJI PRZEZ TELEFON ORAZ ODPOWIEDZI NA ZAPYTANIA KIEROWANE DROGĄ ELEKTRONICZNĄ

1) Udzielanie informacji przez telefon:

a) Pracownik odbiera telefon i przedstawia się imieniem, nazwiskiem oraz podaje nazwę firmy.

b) Pracownik może udzielić informacji **niezawierającej dane osobowe** bez dodatkowej weryfikacji.

c) Pracownik może udzielić informacji **zawierającej dane osobowe** po dokonaniu dodatkowej weryfikacji rozmówcy, czyli zadaniu pytania kontrolnego tj. według okoliczności uzyskanie pewności, że rozmówca jest upoważnioną osobą do uzyskania informacji.

d) Pracownik musi zweryfikować rozmówcę, czy jest to osoba uprawniona w świetle przepisów prawa do pozyskania informacji, o które pyta.

e) Pracownik **NIE UDZIELA TELEFONICZNIE** informacji zawierających dane osobowe **PRACOWNIKOM INSTYTUCJI**.

2) Udzielanie informacji na pytania o dane osobowe przekazane drogą elektroniczną:

a) Pracownik nie udziela informacji zawierających dane osobowe na zewnątrz zakładu pracy pocztą e-mail z zastrzeżeniem lit. b niniejszego punktu, za wyjątkiem komunikacji elektronicznej dostarczonej przez ministra właściwego do spraw informatyzacji (elektroniczna skrzynka podawcza ePUAP).

b) W wypadku otrzymania zapytania e-mailem udzielamy odpowiedzi na piśmie lub drogą e-mailową z zachowaniem procedury korzystania z poczty elektronicznej.

11. PROCEDURA PRZECHOWYWANIA DOKUMENTACJI, W TYM ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI I WYDRUKÓW

1) Zabezpieczenie dokumentacji papierowej:

a) Dokumentację zawierającą dane osobowe przechowujemy w szafach/ szufladach zamykanych na klucz.

b) Dokumentację kadrową należy przechowywać w warunkach zapewniających jej należytą ochronę przed zniszczeniem, najlepiej w szafach metalowych, ogniotrwałych z trwałością min. 2 h zgodnie z wymogiem art. 51n ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

c) Pracownik po zakończeniu pracy chowa wszystkie dokumenty, a klucze do szaf czy szuflad zabiera ze sobą lub zostawia w zabezpieczonym miejscu wiadomym tylko upoważnionym osobom **(tzw. Polityka czystego biurka)**.

d) Jeżeli pracownik opuszcza biuro, pozostawiając je bez nadzoru, każdorazowo zamyka drzwi do pomieszczenia (**nie pozostawiając klucza w zamku.**) Dopuszcza się przekazanie klucza od pomieszczenia pracownikowi z innego pomieszczenia, o ile jego poziom uprawnień jest taki sam lub większy.

e) Pracownik dba, żeby wydruków i kserokopii nie zostawiać w drukarkach, skanerach i kserokopiarkach.

f) Pracownik niszczy dokumenty i tymczasowe wydruki w niszczarce, jak tylko przestają być mu niezbędne do realizacji zadania.

g) ADO oraz upoważnieni przez niego pracownicy są odpowiedzialni za zapewnienie bezpieczeństwa dokumentów i wydruków.

2) Zabezpieczenie elektronicznych nośników informacji:

a) Procedura określa sposób postępowania z nośnikami: twardymi dyskami, płytami CD/DVD, pendrive'ami, telefonami komórkowymi, pamięciami typu „flash" na których znajdują się dane osobowe, celem zabezpieczenia ich przed zniszczeniem, kradzieżą, dostępem osób nieupoważnionych.

b) Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych).

c) Zabrania się wynoszenia poza obszar Spółki wymiennych nośników informacji, a w szczególności twardych dysków z zapisanymi danymi osobowymi bez zgody ADO.

d) Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania (chyba, że z powodu odrębnych przepisów należy je zachować na dłużej).

e) Podlegające likwidacji uszkodzone lub przestarzałe nośniki, a szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny.

f) Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski z danymi osobowymi powinny być wymontowane, zanim zostaną przekazane poza obszar Spółki (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów).

12. PROCEDURA DOSTĘPU DO POMIESZCZEŃ ORAZ POSTĘPOWANIA Z KLUCZAMI

1) Ogólne zasady:

a) Polityka kluczy obejmuje pomieszczenia budynków przy u ul. Żeliwnej 38 w Katowicach.

b) Obowiązuje ośmiogodzinny tryb pracy.

c) Dostęp do pomieszczeń biurowych możliwy jest wyłącznie poprzez wyznaczone do tego drzwi.

2) Nadawanie upoważnień:

a) Udzielenie/anulowanie upoważnienia wymaga wprowadzenia osoby do ewidencji, prowadzonej w postaci elektronicznej przez dedykowany do tego system.

3) Bieżące postępowanie w trakcie dnia pracy:

a) Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane.
b) W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
c) Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu, chyba że pracownik wychodząc zamknął pomieszczenie na klucz.
d) Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w specjalnej skrytce / szufladzie / biurku.
e) Po zakończeniu pracy, pracownicy są zobowiązani do:
   a. wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych (zapisu nie stosuje się wobec administratorów sieci oraz innych osób, których charakter pracy nie pozwala na zastosowanie zapisu);
   b. wyłączenia oświetlenia;
   c. zabezpieczenia i zamknięcia okien i drzwi; iv) aktywacji alarmu
f) Za przestrzeganie w/w zasad bieżących odpowiada ADO lub upoważniony pracownik.

4) Naruszenie zasad polityki kluczy może spowodować wyciągnięcie następujących konsekwencji:

a) Poniesienie odpowiedzialności wynikających z art. 52 *ustawy z dnia 26 czerwca 1974 r. Kodeksu Pracy.*
b) Poniesienie odpowiedzialności wynikających z art. 363 § 1 *ustawy z dnia 23 kwietnia 1964 r. Kodeksu Cywilnego*.

Załącznik nr 1** do Procedury dostępu do pomieszczeń oraz postępowania z kluczami – **REJESTR OSÓB UPOWAŻNIONYCH DO POMIESZCZEŃ

REJESTR OSÓB UPOWAŻNIONYCH DO POMIESZCZEŃ

Lp.	Imię i nazwisko pracownika	Komórka organizacyjna/Stanowisko	Nr pokoju, do którego pracownik ma dostęp

13. PROCEDURA PRZEGLĄDU I PRZECHOWYWANIA DOKUMENTACJI O CHARAKTERZE ARCHIWALNYM

1) Postępowanie w przypadku **dokumentacji niearchiwalnej:**

   a) dokumenty po upływie okresu przechowywania podlegają ocenie ich przydatność w pracy bieżącej,

   b) dokumenty dzieli się na przydatne i nieprzydatne,

   c) dokumentację nieprzydatną niszczy się,

   d) dokumentację przydatną przechowuje się w wydzielonych szafach w działach merytorycznie odpowiedzialnych za dokumenty, aż do ustania przydatności,

   e) oceny dokonuje się nie rzadziej niż raz do roku.

2) Postępowanie w przypadku **dokumentów podlegających archiwizacji:**

   a) Dokumenty należy przechowywać w sposób zapewniający im ochronę przed uszkodzeniem, zniszczeniem lub utratą.

   b) Dokumentację przechowuje się w wydzielonych szafach w działach merytorycznie odpowiedzialnych za dokumenty lub w wyznaczonym pomieszczeniu, aż do ustania czasu przechowywania.

   c) Dostęp do dokumentacji podlegającej archiwizacji powinien być ograniczony do osób merytorycznie odpowiedzialnych za ich składowanie.

   d) Przedstawiciel ADO lub osoba przez niego upoważniona raz na rok dokonuje przeglądu i wydzielenia dokumentacji o charakterze archiwalnym.

   e) W przypadku dokumentacji archiwalnej, której czas przechowywania upłynął (np. akta pracownicze), przedstawiciel jednostki winien skierować pismo do archiwum państwowego celem wyrażenia zgody na brakowanie dokumentacji.

14. PROCEDURA POSTĘPOWANIA Z BRUDNOPISAMI/ NISZCZENIE ZBĘDNYCH DOKUMENTÓW

1) Dokumenty zawierające dane osobowe należy wyrzucać w stopniu zniszczenia uniemożliwiającym odczytanie z nich danych. Dokumenty przed wyrzuceniem należy zniszczyć za pomocą niszczarki o odpowiedniej dla klasy dokumentów normie. Klasę (normę) niszczarki zatwierdza IOD w momencie potrzeby zakupu niszczarki.

2) Notatki i pliki służące do wytwarzania dokumentów są przechowywane i zabezpieczone tak, jak dokumenty, do których wytworzenia służą.

3) Pliki, które powstały w systemach informatycznych w celu zbudowania dokumentów papierowych, powinny zostać zdepersonalizowane lub usunięte w momencie zatwierdzenia ostatecznej wersji dokumentu i jego wydrukowaniu.

4) Dokumenty zawierające dane osobowe powinny mieć włączone rejestrowanie zmian w celu zapewnienia zasady rozliczalności.

5) Jeżeli zachodzi konieczność zniszczenia większej ilości dokumentów zawierających dane osobowe, można przekazać je firmie zajmującej się brakowaniem dokumentacji, po uprzednim podpisaniu umowy zawierającej regulacje dot. przetwarzania danych osobowych.

15. PROCEDURA KORZYSTANIA ZE SPRZĘTU SŁUŻBOWEGO: TELEFON KOMÓRKOWY, LAPTOP, NOŚNIKI DANYCH

1) Przed rozpoczęciem pracy na sprzęcie należącym do ADO pracownik podpisuje oświadczenie o odpowiedzialności za powierzony sprzęt, tzw. protokół zdawczo odbiorczy.

2) Sprzęt służbowy może być wynoszony poza zakład pracy tylko za zgodą ADO. Taki sprzęt musi posiadać dodatkowe zabezpieczenia w postaci szyfrowanych dysków twardych. Odpowiedni rejestr w tym zakresie jest prowadzony przez ADO/upoważnionego pracownika. (Załącznik nr 1 do niniejszej Procedury.)

3) Pracownik może używać powierzonego sprzętu jedynie w celach służbowych, o ile inny dokument lub ustalenia z pracodawcą nie dopuszczają takiej możliwości.

4) W związku z korzystaniem ze sprzętu służbowego, pracownik nie może zapisywać numerów osób fizycznych w telefonie prywatnym oraz wykorzystywać prywatnego telefonu do celów służbowych.

5) Jedynie służbowe, zarejestrowane pendrive'y oraz inne nośniki danych mogą być używane do pracy. Nie wolno posługiwać się prywatnymi nośnikami danych.

6) Podczas pracy na sprzęcie służbowym oraz podczas jego transportu, stosuje się odpowiednio procedury korzystania z sieci Internet, procedury transportu dokumentów oraz innych procedur.

Załącznik nr 1 *do Procedury korzystania ze sprzętu służbowego -* ***REJESTR SPRZĘTU SŁUŻBOWEGO, W TYM REJESTR NOŚNIKÓW DANYCH***

REJESTR SPRZĘTU SŁUŻBOWEGO W TYM REJESTR NOŚNIKÓW DANYCH

Lp.	Imię i nazwisko pracownika, któremu powierzono sprzęt służbowy	Rodzaj sprzętu	Nr inwentaryzacyjny	*wew. – wewnętrzny – możliwość używania wyłącznie na terenie zakładu pracy, zew. – zewnętrzny – możliwość używania również poza zakładem pracy.	Czy sprzęt/nośnik posiada możliwość szyfrowania danych (TAK/NIE)
1					
2					

16. PROCEDURA WYKONANIA SPRAWDZENIA W PODMIOCIE PRZETWARZAJĄCYM, Z KTÓRYM ZAWARTA ZOSTAŁA UMOWA

1) W celu sprawdzenia zgodności przetwarzania danych w firmie (podmiocie przetwarzającym), z którą zawarta została umowa powierzenia przetwarzania danych, należy przeprowadzić audyt zastosowanych zabezpieczeń.

2) Środki audytowe, które mogą być wykorzystane do zweryfikowania zastosowanych przez podmiot przetwarzający środków zabezpieczających dane to:

a) spotkanie audytowe w miejscu przetwarzania danych osobowych;
b) ankieta audytowa;
c) spotkanie audytowe on-line.

3) Audyt zgodności przetwarzania danych przeprowadza IOD lub pracownik wyznaczony przez ADO.

4) Po przeprowadzonym audycie przygotowany zostaje raport pokontrolny, który przedstawiany jest podmiotowi przetwarzającemu oraz ADO.

5) Podmiot przetwarzający zobowiązany jest ustosunkować się do zaleceń wskazanych przez osobę wykonującą audyt.

17. INSTRUKCJA POSTĘPOWANIA W PRZYPADKU WYSTĄPIENIA NARUSZENIA OCHRONY DANYCH

1) Niniejsza Instrukcja określa zasady postępowania pracowników przy przetwarzaniu danych osobowych w przypadku naruszenia bezpieczeństwa tych danych.

2) Każdy pracownik Spółki w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego lub IOD.

3) Naruszeniem zabezpieczenia danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub usunięcia tych danych, a w szczególności:

   a) nieautoryzowany dostęp do danych,

   b) nieautoryzowane modyfikacje lub zniszczenie danych,

   c) udostępnienie danych nieautoryzowanym podmiotom,

   d) nielegalne ujawnienie danych,

   e) pozyskiwanie danych z nielegalnych źródeł.

4) W przypadku stwierdzenia naruszenia zabezpieczeń lub zaistnienia sytuacji, które mogą wskazywać na naruszenie zabezpieczenia danych osobowych, każdy pracownik zatrudniony przy przetwarzaniu danych osobowych jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie zgłosić ten fakt bezpośredniemu przełożonemu oraz IOD, a następnie postępować stosownie do podjętej przez niego decyzji.

5) Zgłoszenie naruszenia zabezpieczeń danych osobowych powinno zawierać:

   a) opisanie symptomów naruszenia zabezpieczeń danych osobowych,

   b) określenie sytuacji i czasu w jakim stwierdzono naruszenie zabezpieczeń danych osobowych,

   c) określenie wszelkich istotnych informacji mogących wskazywać na przyczynę naruszenia,

   d) określenie znanych danej osobie sposobów zabezpieczenia systemu oraz wszelkich kroków podjętych po ujawnieniu zdarzenia.

6) IOD lub inna upoważniona przez ADO osoba, podejmuje wszelkie działania mające na celu:

   a) minimalizację negatywnych skutków zdarzenia,

   b) wyjaśnienie okoliczności zdarzenia,

   c) zabezpieczenie dowodów zdarzenia,

   d) umożliwienie dalszego bezpiecznego przetwarzania danych.

7) W celu realizacji zadań wynikających z niniejszej instrukcji IOD lub inna upoważniona przez ADO osoba, ma prawo do podejmowania wszelkich działań dopuszczonych przez prawo, a w szczególności:

   a) żądania wyjaśnień od pracowników,

   b) korzystania z pomocy konsultantów,

   c) nakazania przerwania pracy, zwłaszcza w zakresie przetwarzania danych osobowych.

8) Polecenia IOD lub innej upoważnionej przez ADO osoby, wydawane w celu realizacji zadań wynikających z niniejszej instrukcji są priorytetowe i winny być wykonywane przed innymi poleceniami, zapewniając ochronę danych osobowych.

9) Odmowa udzielenia wyjaśnień lub współpracy z IOD lub inną upoważnioną przez ADO osobą, traktowana będzie jako naruszenie obowiązków pracowniczych.

10) Natychmiast po stwierdzeniu naruszenia ochrony danych osobowych ADO powinien zgłosić to organowi nadzorczemu bez zbędnej zwłoki, jeżeli jest to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że IOD jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli nie można dokonać zgłoszenia w terminie 72 godzin, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki. IOD prowadzi rejestr naruszeń ochrony danych. Wzór rejestru incydentów/naruszeń stanowi *Załącznik nr 1* do niniejszej Instrukcji.

11) Zgłoszenie naruszenia powinno:

   a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorię i przybliżoną liczbę osób, których dane dotyczą;

   b) zawierać dane osobowe IOD lub dane kontaktowe do ADO;

   c) opisywać możliwe konsekwencje naruszenia ochrony danych;

   d) opisywać środki zastosowane lub zaproponowane przez IOD w celu zaprzestania naruszenia przepisów w zakresie ochrony danych osobowych oraz zminimalizowania jego negatywnych skutków.

12) Po zażegnaniu sytuacji naruszającej bezpieczeństwo danych osobowych IOD sporządza protokół z naruszenia bezpieczeństwa informacji, w którym przedstawia przyczyny i skutki zdarzenia oraz wnioski, w tym kadrowe, ograniczające możliwość wystąpienia zdarzenia w przyszłości. Wzór protokołu stanowi *Załącznik nr 2* do niniejszej Instrukcji.

13) Nieprzestrzeganie zasad postępowania określonych w niniejszej Instrukcji stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej.

Załącznik nr 1** do Instrukcji postępowania w przypadku wystąpienia incydentu/naruszenia –* ***REJESTR INCYDENTÓW/NARUSZEŃ

REJESTR NARUSZEŃ/INCYDENTÓW

Opis incydentu/naruszenia	Źródło zgłoszenia	Data wykrycia incydentu/naruszenia	Data zgłoszenia do ADO	Opis procedury naprawczej	Data zgłoszenia do UODO	Skutki

Załącznik nr 2 *do Instrukcji postępowania w przypadku wystąpienia incydentu -* ***WZÓR PROTOKOŁU Z NARUSZENIA BEZPIECZEŃSTWA INFORMACJI***

WZÓR PROTOKOŁU Z NARUSZENIA BEZPIECZEŃSTWA INFORMACJI

Data: ..... Godzina: .....

1. Osoba powiadamiająca o zaistniałym zdarzeniu (imię, nazwisko, stanowisko służbowe, identyfikator użytkownika - jeśli występuje):

.....
.
.....

2. Lokalizacja zdarzenia (np. nr pokoju, nazwa pomieszczenia):

.....
.
.....

3. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....
.
.....

4. Podjęte działania:

.....
.
.....

5. Przyczyny wystąpienia zdarzenia:

.....
.
.....

6. Postępowanie wyjaśniające:

.....

.....

.....

(podpis IOD)

18. INSTRUKCJA UDOSTĘPNIANIA DANYCH OSOBOWYCH NA WNIOSEK

1) Udostępnianie danych osobowych odbywa się zawsze na pisemny wniosek. Wzór Wniosku o udostępnienie danych stanowi *Załącznik nr 1* do Instrukcji udostępniania danych.

2) Po zarejestrowaniu wniosku należy przekazać go do zaopiniowania do IOD, który sprawdza czy istnieje możliwość udostępnienia danych oraz weryfikuje czy wniosek zawiera odpowiednie podstawy formalne udostępnienia oraz czy jest poprawnie skonstruowany.

3) Po zaopiniowaniu wniosku i przygotowaniu odpowiedzi IOD wprowadza wniosek do rejestru udostępnień.

4) Wzór rejestru stanowi ***Załącznik nr 2*** do niniejszej instrukcji.

5) Rejestr prowadzony jest w formie elektronicznej.

6) Odbiór wnioskowanych dokumentów jest możliwy w godzinach i dniach pracy ADO.

7) Wydanie wnioskowanej dokumentacji musi zostać potwierdzone podpisem wydającego i odbierającego oraz datą wydania na złożonym wniosku.

8) Dokumentacja może także zostać przesłana pocztą (przesyłką poleconą za potwierdzeniem odbioru) na wskazany przez wnioskodawcę adres.

Załącznik nr 1 *do Instrukcji udostępniania danych* - ***WNIOSEK O UDOSTĘPNIENIE DANYCH***

WNIOSEK O UDOSTĘPNIENIE DANYCH

1. Wniosek do:

.....

.....(adres)

KRS: ..... NIP: ..... REGON: .....

2. Wnioskodawca:

.....

.....

(nazwisko i imię lub nazwa/siedziba, adres zamieszkania)

3. Podstawa prawna upoważniająca wnioskodawcę do przetwarzania danych osobowych:

.....

.....

(w przypadku wnioskowania przez właściciela danych osobowych podstawy prawnej nie wpisujemy,wpisać należy tylko: właściciel danych)

4. Wskazanie przeznaczenia dla udostępnionych danych:

.....

.....

(cel przetwarzania danych: w jakiej sprawie potrzebne są wnioskowane informacje/do jakiej instytucji)

5. Zakres danych, które mają zostać udostępnione:

.....

.....

(informacje, jakie mają zostać udostępnione, rodzaj dokumentu jaki ma zostać wydany, w jakiej formie)

6. Informacje umożliwiające wyszukanie danych w zbiorze:

.....

.....

(imię i nazwisko osoby, której dane dotyczą, data urodzenia/nr paszportu/adres zamieszkania)

.....

(Data i podpis osoby wnioskującej lub upoważnionej)

Załącznik nr 2** do Instrukcji udostępniania danych osobowych na wniosek – **REJESTR UDOSTĘPNIEŃ

REJESTR UDOSTĘPNIEŃ

Nazwa podmiotu, któremu dane udostępniono	Data wpływu wniosku	Data udostępnienia	Podstawa prawna udostępnienia	Zakres udostępnionych danych	Dane osobowe

19. INSTRUKCJA ZAWIERANIA UMOWY POWIERZENIA

1) Przed zawarciem umowy z podwykonawcą przetwarzającym dane, których Administratorem jest ŚFR. należy sporządzić umowę powierzenia. Wzór umowy powierzenia stanowi *Załącznik nr 1* do niniejszej instrukcji.

2) Dopuszcza się zastosowanie innego wzoru umowy powierzenia przetwarzania danych niż ujęty w *Załączniku nr 1* do niniejszej instrukcji, po ówczesnej akceptacji przez IOD.

3) Przed podpisaniem umowy z podwykonawcą, dokumentacja musi zostać zaopiniowana pod kątem ochrony danych osobowych przez IOD.

4) Dane z umów wprowadzane są przez osobę do tego wyznaczoną do Rejestru umów, który stanowi *Załącznik nr 2* do niniejszej instrukcji.

5) Umowy powierzenia muszą być zawierane z podmiotami obsługującymi ADO w zakresie np.: serwisu kopiarek, hostingu, obsługi informatycznej, niektórych ubezpieczeń grupowych, obsługi BHP, usług archiwizacji.

6) Za podpisanie umowy powierzenia odpowiedzialny jest przedstawiciel Spółki/wyznaczony pracownik koordynujący zawierane przez Spółkę umowy.

Załącznik nr 1** do Instrukcji zawierania umowy powierzenia - **UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

zawarta w dniu ..... w ..... pomiędzy:
..... z siedzibą w ....., ul. .....,
NIP ....., REGON ..... reprezentowaną przez:
Pana/Panią ..... – .....,
zwaną/ym dalej **„Administratorem"** lub **"Zleceniodawca"** lub „**Stroną**"
a

..... z siedzibą w ....., ul. .....,
NIP ....., REGON ..... reprezentowaną przez:
Pana/Panią ..... – .....,
zwaną/ym dalej **„Przetwarzającym**" lub **"Zleceniobiorcą"** lub „**Stroną**"
zwanymi dalej łącznie: „**Stronami**"; o następującej treści:

§1

Definicje

Ilekroć w niniejszej umowie powierzenia przetwarzania danych osobowych mowa o:

1. „**administratorze danych**" – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
2. „**danych osobowych**" – rozumie się przez to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą");
3. „**przetwarzaniu danych**" – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
4. „**systemie informatycznym**" – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
5. „**Umowie**" – rozumie się przez to niniejszą umowę powierzenia przetwarzania danych osobowych.

§2 Oświadczenia

Stron

Strony oświadczają, co następuje:

1. Zleceniodawca oświadcza, iż jest administratorem danych osobowych wskazanych w §4 oraz, że spełnił warunki legalności przetwarzania danych osobowych, przewidzianych w obowiązujących przepisach prawa.

Przetwarzający

2. oświadcza, że znane są mu regulacje powszechnie obowiązującego prawa dotyczące ochrony danych osobowych, w tym ustawa z dnia 10 maja 2018 roku o ochronie danych osobowych (Dziennik Ustaw z 2018 roku, pozycja numer 1000, dalej jako: Ustawa) oraz Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dziennik Urzędowy Unii Europejskiej L numer 119, strona 1, dalej jako: RODO) oraz iż regulacje te stosuje i będzie stosował przez cały okres obowiązywania niniejszej Umowy.

3. Przetwarzający oświadcza, że zapewnia obecnie i będzie zapewniał przez cały okres obowiązywania niniejszej Umowy, wystarczające gwarancje, w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby, wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie danych osobowych spełniało wymogi powszechnie obowiązującego prawa, w tym Ustawy i RODO oraz aby chroniło prawa osób, których dane osobowe dotyczą.

4. Przetwarzający oświadcza, iż urządzenia i systemy informatyczne służące do przetwarzania powierzonych mu danych osobowych są zgodne z wymogami obowiązujących przepisów prawa.

§3

Przedmiot Umowy

1. Administrator powierza Przetwarzającemu do przetwarzania dane osobowe, a
   Przetwarzający zobowiązuje się do ich przetwarzania zgodnie z prawem i Umową.

2. Przetwarzający przetwarzać będzie dane osobowe w siedzibie i systemach
   ..... (*wpisać stan faktyczny: Administrator - Przetwarzający*).

3. Przetwarzający może przetwarzać dane osobowe wyłącznie w zakresie i celu przewidzianych w §4.

§4

Zakres i cel przetwarzania danych osobowych

1. Zakres przetwarzanych danych osobowych ..... (*wpisać kategorię osób*) Administratora obejmuje niezbędne dane osobowe wynikające z Umowy głównej z dnia ..... nr ..... dot. ..... (dalej jako: Umowa główna).

2. Administrator powierza Przetwarzającemu do przetwarzania dane osobowe konieczne do prawidłowej realizacji przedmiotu Umowy głównej, a w szczególności:

   1) .....
   2) .....
   3) .....

3. Celem przetwarzania danych osobowych jest realizacja przedmiotu Umowy głównej, a w szczególności:

   1) .....
   2) .....
   3) .....

§5

Zasady przetwarzania danych osobowych

1. Przy przetwarzaniu danych osobowych związanych z wykonaniem Umowy głównej, Przetwarzający powinien przestrzegać zasad wskazanych w niniejszym paragrafie oraz w Ustawie i RODO.

2. Dane stanowiące przedmiot niniejszej Umowy nie będą podlegały profilowaniu tj. nie będą poddawane dowolnemu zautomatyzowanemu przetwarzaniu danych osobowych pozwalającemu ocenić czynniki osobowe osoby fizycznej – nie będą one przetwarzane w sposób zautomatyzowany, w sposób, który wywołuje wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób znacząco na nią wpływa.

3. Przed rozpoczęciem przetwarzania danych osobowych Przetwarzający jest zobowiązany do podjęcia środków zabezpieczających dane osobowe, a w szczególności musi:

   1) zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku związanym z przetwarzaniem danych osobowych, a przede wszystkim powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem obowiązujących przepisów prawa oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;

   2) dopuszczać do przetwarzania danych osobowych wyłącznie osoby posiadające wydane przez niego imienne upoważnienie. Administrator upoważnia Przetwarzającego do udzielenia ww. upoważnień;

   3) prowadzić ewidencję osób zatrudnionych przy przetwarzaniu danych osobowych przetwarzanych w związku z wykonywaniem Umowy głównej. Przetwarzający, na żądanie Administratora, jest zobowiązany przedstawić aktualną listę osób z przyznanym dostępem do danych osobowych;

   4) zapewnić, aby osoby mające dostęp do przetwarzania danych osobowych zachowały je oraz sposoby zabezpieczeń w tajemnicy, przy czym obowiązek zachowania tajemnicy istnieje również po zakończeniu Umowy głównej oraz ustaniu zatrudnienia u Przetwarzającego.

4. Przekazywanie danych osobowych odbywać się będzie pomiędzy Stronami w sposób zapewniający ich należytą ochronę i zabezpieczenie przed osobami nieupoważnionymi.

5. Przetwarzający powiadomi Administratora niezwłocznie o wszystkich naruszeniach dotyczących przetwarzania danych osobowych stanowiących przedmiot niniejszej Umowy, na adres mailowy wskazany w § 12, nie później niż w terminie 24 godzin od wystąpienia

Przetwarzający

naruszenia. Przetwarzający jest zobowiązany pomagać Administratorowi ustalić stan faktyczny oraz współpracować w celu podjęcia działań naprawczych.

6. Przetwarzający dokumentuje wszelkie naruszenia, w tym okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze.

7. nie jest uprawniony do przekazywania informacji o naruszeniu jakimkolwiek innym podmiotom, w szczególności organowi nadzorczemu.

8. W trakcie trwania Umowy głównej dopuszczalna jest pseudonimizacja zarówno przez Przetwarzającego na podstawie Umowy, jak i podmiot, któremu dane zostały podpowierzone.

9. Administrator zobowiązuje Przetwarzającego do powiadomienia każdorazowo, jeżeli wydane mu polecenie stanowi naruszenie RODO lub innych przepisów o ochronie danych drogą mailową na adres wskazany w § 12 ust. 1.

10. Przetwarzający może zwracać się do Administratora o udzielenie wytycznych dotyczących wykonywania niniejszej Umowy. Administrator jest zobowiązany udzielać Przetwarzającemu wytycznych w terminie określonym w § 5 ust. 9 Umowy.

11. Administrator jest zobowiązany do udzielenia Przetwarzającemu wytycznych tak szybko, jak to możliwe, jednakże nie później niż w terminie 7 dni od dnia skierowania prośby w tym zakresie przez Przetwarzającego.

12. Przetwarzający jest związany wytycznymi i informacjami udzielonymi przez Administratora dotyczącymi wykonywania niniejszej Umowy, o ile nie są sprzeczne z literą prawa.

13. Administrator jest zobowiązany do współdziałania z Przetwarzającym w celu wykonywania niniejszej Umowy w sposób zapewniający należyty poziom ochrony praw osób, których dane osobowe dotyczą.

§6

Uprawnienia kontrolne Administratora

1. Administrator ma prawo do przeprowadzenia kontroli przestrzegania przez Przetwarzającego zasad przetwarzania danych osobowych.

2. Kontrole, o których mowa w ust. 1, mogą być wykonywane przez Administratora (osoby przez niego wyznaczone) w miejscu przetwarzania danych osobowych w dni robocze w godzinach pracy Przetwarzającego.

3. Administrator jest zobowiązany do przeprowadzania kontroli w taki sposób, aby nie utrudniać Przetwarzającemu prowadzenia jego działalności ponad potrzebę.

4. Przetwarzający udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków wynikających z przedmiotu niniejszej Umowy oraz RODO.

5. Przetwarzający zapewni również w umowie powierzenia z dalszym podmiotem przetwarzającym możliwość realizacji przez Administratora bezpośredniej kontroli względem dalszego podmiotu przetwarzającego.

§7

Usunięcie danych osobowych

1. Najpóźniej w ciągu 30 dni licząc od daty rozwiązania bądź wygaśnięcia Umowy głównej, Przetwarzający jest zobowiązany zwrócić, w uzgodnionym między Stronami formacie, dane, które przetwarzał w związku z wykonywaniem Umowy głównej, a następnie usunąć je ze wszystkich nośników informacji, o ile postanowienia innych umów związanych z niniejszą Umową lub przepisy prawa nie stanowią inaczej.

2. Przez usunięcie danych, o którym mowa w ust. 1, rozumieć należy takie zniszczenie, które nie pozwoli na ich ponowne odtworzenie.

3. Przetwarzający na pisemną prośbę Administratora w ciągu 30 dni, licząc od dnia rozwiązania bądź wygaśnięcia Umowy głównej, potwierdza w formie pisemnej wywiązanie się z postanowień zawartych w ust. 1 i ust. 2.

4. Treść niniejszego paragrafu nie stoi na przeszkodzie wykonaniu przez Przetwarzającego obowiązków wynikających z obowiązujących przepisów prawa, w tym obowiązków sprawozdawczych.

§8

Odpowiedzialność Przetwarzającego

1. Przetwarzający odpowiada za szkody, jakie powstaną u Administratora lub osób trzecich w wyniku niezgodnego z Umową i przepisami prawa przetwarzania przez Przetwarzającego powierzonych mu danych osobowych.

2. W przypadku, w którym Administrator będzie ponosił odpowiedzialność związaną z przetwarzaniem danych osobowych przez Przetwarzającego, Przetwarzający jest zobowiązany do zwolnienia Administratora z tej odpowiedzialności.

3. Jeżeli wystąpi sytuacja, o której mowa w ust. 2, Przetwarzający będzie zobowiązany do uiszczenia takiego odszkodowania lub kary pieniężnej w terminie i w sposób wskazany przez Administratora.

§9

Czas trwania Umowy

1. Umowa zostaje zawarta na czas .....

2. Administrator jest uprawniony do rozwiązania Umowy ze skutkiem natychmiastowym w przypadku, gdy:

   1) organy administracji publicznej odpowiedzialne za nadzór nad przestrzeganiem zasad przetwarzania danych osobowych stwierdzą, że Przetwarzający nie przestrzega tych zasad;

   2) Administrator, w wyniku przeprowadzenia kontroli, o której mowa w § 6 Umowy stwierdzi, że Przetwarzający nie przestrzega zasad przetwarzania danych osobowych wynikających z Umowy lub obowiązujących przepisów prawa.

§10

Przetwarzający

Dalsze powierzenie danych osobowych

1. Przetwarzający jest uprawniony do dokonania podpowierzenia na rzecz podmiotów wskazanych w Załączniku nr 1 do Umowy.

2. informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia podmiotów wskazanych w Załączniku nr 1 nie później niż w terminie 14 dni przed ich wprowadzeniem, a Administrator w tym terminie może wnieść sprzeciw wobec takich zmian, w którym wyjaśni podstawy do nieudzielenia akceptacji nowemu podmiotowi. Wniesienie sprzeciwu oznacza brak zgody na dodanie lub zastąpienie takiego podmiotu. W takim przypadku Stronom przysługuje prawo rozwiązania Umowy oraz zakończenia współpracy ze skutkiem natychmiastowym.

3. Podpowierzenie jest dopuszczalne tylko na podstawie umowy powierzenia.

4. Przetwarzający może korzystać wyłącznie z usług takich dalszych podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

5. Za naruszenia oraz ich konsekwencje występujące u podmiotu, któremu Przetwarzający powierzył dane osobowe stanowiące przedmiot niniejszej Umowy, odpowiada Przetwarzający. Przetwarzający jest zobowiązany do poinformowania Administratora o takich naruszeniach zgodnie z § 5 ust. 5 Umowy.

6. W przypadku, gdy Przetwarzający zamierza dokonać podpowierzenia na rzecz podmiotu z państwa trzeciego, musi uzyskać uprzednią pisemną szczegółową zgodę Administratora.

§11

1. Przetwarzający zobowiązuje się do zachowania w tajemnicy wszelkich informacji dotyczących zawarcia oraz wykonania Umowy głównej, jak również informacji dotyczących Administratora oraz działalności prowadzonej przez Administratora, w których posiadanie wszedł w związku z zawarciem lub wykonaniem Umowy głównej.

2. Przetwarzający zapewnia, że wszystkie osoby mające dostęp w związku z zawarciem lub wykonaniem przez Przetwarzającego Umowy głównej do informacji, o których mowa w ust. 1, w tym: pracownicy Przetwarzającego, osoby i podmioty pozostające z Przetwarzającym w stosunku zlecenia lub innym stosunku prawnym o podobnym charakterze oraz inne osoby lub podmioty, które z racji czynności wykonywanych na rzecz Przetwarzającego muszą mieć zapewniony dostęp do takich informacji, zostaną zobowiązane do zachowania tych informacji w tajemnicy.

§12

Adresy Stron i dane osób

1. Wszelka korespondencja w sprawach związanych z Umową będzie kierowana na podane niżej adresy Stron:

   1) **Do Przetwarzającego:** adres: ....., tel.: ....., e-mail: .....

2) **Do Administratora:** adres: ....., tel.: ....., e-mail: .....

2. Przetwarzającego w kontaktach z Administratorem, w zakresie ustaleń Umowy reprezentuje.....

3. Administratoraw kontaktach z Przetwarzającym, w zakresie ustaleń Umowy reprezentuje .....

4. Zmiana adresów i danych osób, o których mowa w ust. 1 – 3, nie stanowi zmiany Umowy. O każdej zmianie powyższych danych Strony powiadomią się na piśmie, za potwierdzeniem odbioru lub drogą elektroniczną.

§13

Klauzula salwatoryjna

1. Jeżeli na skutek sprzeczności z prawem lub z zasadami współżycia społecznego lub z uwagi na obejście prawa lub z jakiegokolwiek innego powodu, nieważnością będzie dotknięta tylko część niniejszej Umowy, Umowa pozostaje w mocy co do pozostałych części, chyba że z okoliczności wynika, iż bez postanowień dotkniętych nieważnością niniejsza Umowa nie zostałaby zawarta.

2. W przypadku, o którym mowa w ust. 1, Strony zobowiązują się niezwłocznie uzgodnić nową treść postanowień Umowy dotkniętych nieważnością, która w najpełniejszym zakresie będzie odzwierciedlała zamiary i intencje Stron.

§14

Postanowienia końcowe

1. Wszelkie zmiany w treści Umowy wymagają formy pisemnej pod rygorem nieważności, z zastrzeżeniem przypadków wymienionych w Umowie.

2. W zakresie nieuregulowanym w niniejszej Umowie zastosowanie będą miały przepisy powszechnie obowiązującego prawa, w tym Ustawy i RODO.

3. Sądem właściwym do rozstrzygnięcia sporów związanych z Umową będzie sąd właściwy miejscowo dla siedziby Administratora.

4. Umowa została sporządzona w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Administrator	**Przetwarzający**
podpis i pieczęć	*podpis i pieczęć*

Załącznik nr 1

Lista podmiotów, którym Przetwarzający podpowierza przetwarzanie danych osobowych

l.p.	Nazwa podmiotu	Adres podmiotu	NIP

Załącznik nr 2 *do Instrukcji zawierania umowy powierzenia* ***- REJESTR PODMIOTÓW TRZECICH***

REJESTR PODMIOTÓW TRZECICH

Nazwa podmiotu	Cel przetwarzania danych	Data rozpoczęcia umowy	Data zakończenia umowy	Dodatki do umowy

20. REJESTR CZYNNOŚCI PRZETWARZANIA

Informacje o Administratorze: .....
Dane kontaktowe Inspektora Ochrony Danych: .....

Nazwa dokumentu	Osoba, która ma dostęp do dokumentu wewnątrz jednostki	Opis celu przetwarzania	Kategorie osób, których dane dotyczą	Kategorie danych osobowych	Odbiorcy danych	Planowany termin usunięcia danych	Opis środków bezpieczeństwa	Podstawa prawna	Nazwa zbioru danych

21. PROCEDURA KONTROLI SYSTEMU OCHRONY DANYCH OSOBOWYCH

1) Celem procedury jest uporządkowanie i przedstawienie czynności związanych z kontrolą stanu bezpieczeństwa danych osobowych.

2) Procedura obejmuje wszystkie procesy organizacji, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.

3) Do kontroli stanu ochrony danych osobowych upoważniony jest IOD, wyznaczeni kontrolerzy wewnętrzni oraz Zarząd.

4) Kontroli podlegają: systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo działań względem danych osobowych podejmowanych przez pracowników oraz zgodność stanu faktycznego z wymaganiami RODO.

5) Inspektor Ochrony Danych przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe. Plan kontroli jest zatwierdzany przez ADO. Kontrola może mieć formę stacjonarnej weryfikacji stanu bezpieczeństwa lub wywiadu lub ankiet bezpieczeństwa i powinna odbyć się co najmniej raz w roku.

6) Po dokonanej kontroli osoba ją przeprowadzająca przygotowuje i przekazuje raport pokontrolny stanowiący Załącznik 1 do niniejszej Procedury Administratorowi Danych Osobowych. Na jego podstawie ADO inicjuje działania korygujące lub zapobiegawcze.

Załącznik 1 *do Procedury kontroli systemu ochrony danych osobowych*

Raport pokontrolny ODO	Sporządził:	
	Data:	
	Ilość stron	

Raport nr: .....

Miejsce kontroli: Kierownik kontrolowanego obszaru: Osoba(y) kontrolowana(e):	Termin wykonania kontroli: Godzina rozpoczęcia: Godzina zakończenia:
Kontrolerzy:	Kontrolowany obszar:

Podstawa audytu (zaznacz właściwe):

- planowana kontrola - kontrola specjalna - kontrola sprawdzająca

Zakres	Obserwacja/Pole doskonalenia/Mała niezgodność/Duża niezgodność/Zalecenie O/PD/MN/DN/Z

22. PROCEDURA POSTĘPOWANIA W ZAKRESIE ANALIZY RYZYKA

1) Definicje:

a) **Aktywa** - środki materialne i niematerialne mające wpływa na przetwarzanie danych osobowych;
b) **Zagrożenie** - potencjalne naruszenie (potencjalny incydent);
c) **Skutki** - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia);
d) **Ryzyko** - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.

2) Analiza Ryzyka pozwala na określenie odpowiednich - adekwatnych do przetwarzanych danych, środków technicznych i organizacyjnych w celu zabezpieczenia danych przed niepowołanym dostępem. Analizę należy przeprowadzić zgodnie z poniżej opracowaną metodyką.

3) Metodyka szacowania ryzyka:

Podstawowym kryterium oceny ryzyk jest eliminacja ryzyk o maksymalnej wartości z obszarów o największym ryzyku oraz eliminowanie ryzyk związanych z niezgodnością z regulacjami prawnymi.

Na podstawie wyników analizy ryzyka opracowywane są plany postępowania z ryzykiem dla zagrożeń o ryzyku większym niż ustalony poziom ryzyka akceptowalnego oraz dla zagrożeń związanych z niezgodnością z przepisami prawa. Analiza ryzyka jest przeprowadzana regularnie, nie rzadziej niż raz do roku. Analiza ryzyka jest przeprowadzana również po wprowadzeniu zmian mających wpływ na ochronę danych osobowych w jednostce.

(F) Częstotliwość: mniej niż raz w roku, raz w roku, raz w miesiącu, raz w tygodniu, codziennie.
(O) Prawdopodobieństwo: nieistotne (pomijalne), mało prawdopodobne, możliwe (wyobrażalne), możliwe (wyobrażalne), zwykłe.
(A) Możliwość uniknięcia: oczywista, prawdopodobna, możliwa, niezbyt realna, niemożliwa.

Klasy konsekwencji zdarzenia		
Klasa	**Wskazanie**	**Skutek**
C1	Nieznaczne	nie ma wpływu
C2	Marginalne	powoduje krótkie przerwy w pracy, utratę mało istotnych danych
C3	Poważne	powoduje dłuższe przerwy w pracy, utrata danych istotnych lecz nie kluczowych
C4	Bardzo poważne	powoduje ponad dobowy przestój w pracy, utratę danych kluczowych

P=F+O+A	Zapobieganie/Konsekwencje				
	P				
Klasy konsekwencji zdarzenia	3-4	5-7	8-10	11-13	14-15
C1	1	2	3	4	5
C2	2	3	4	5	6
C3	3	4	5	6	7
C4	4	5	6	7	8

Ocena ryzyka	
	transferowe
	monitorowane
	akceptowalne

4) Plan postępowania z ryzykiem:

UNIKANIE

Unikanie ryzyka zakłada konieczność podjęcia działań mających na celu zmodyfikowanie bądź zaprzestanie aktywności powodującej powstawanie określonych zagrożeń. To unikanie przez organizację działań, które powodują powstanie określonych typów ryzyka, np. w przypadku gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatny do zysków.

ZACHOWANIE

Świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu organizacji (zabezpieczeń), jeżeli poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka.

MODYFIKOWANIE

Polega na obniżeniu poziomu ryzyka (np. poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszenie skutków jego wystąpienia). Proces zarządzania ryzykiem polega na modyfikowaniu ryzyk przekraczających akceptowalny próg. Jest on często nazywany „łagodzeniem ryzyka", „minimalizacją ryzyka", „eliminacją ryzyka", „zapobieganiem ryzyku" lub „redukcją ryzyka", z zależności od sposobów postępowania z ryzykiem. Mogą być one następujące:

a) uniknięcie ryzyka dzięki decyzji o nierozpoczynaniu lub niekontynuowaniu działań powodujących ryzyko,
b) podjęcie lub zwiększenie ryzyka w celu wykorzystania szansy,
c) usunięcie źródła ryzyka,
d) zmiana prawdopodobieństwa,
e) zmiana następstw,
f) dzielenie ryzyka wraz z inną stroną (innymi stronami),
g) zachowanie ryzyka na podstawie świadomej decyzji.

Zaleca się wybranie takiego wariantu lub takich wariantów, które zapewnią znaczną redukcję ryzyka przy względnie małych nakładach. Przy wybieraniu wariantów nie trzeba ograniczać się tylko do jednego, gdyż często okazuje się, że korzystne jest wybranie np. zmiany prawdopodobieństwa oraz zmiany następstw.

DZIELENIE

Przeniesienie ryzyka na inny podmiot przy wykorzystaniu mechanizmów prawnych oraz działań o charakterze organizacyjnym czy zabezpieczającym. Przykładem stosowania tej metody jest przykład dzierżawcy, który zawarł długoterminową umowę dzierżawy z klauzulą stałego czynszu przenosząc ryzyko inflacji na właściciela nieruchomości, wykupienie ubezpieczenia od jakiegoś zdarzenia lub scedowanie skutków ryzyka na inny podmiot.

5) Wszędzie, gdzie Administrator decyduje się modyfikować ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne.
6) Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.
7) Analiza ryzyka prowadzona jest w wersji elektronicznej.

8) Analizę ryzyka należy minimum raz w roku aktualizować. Dodatkowo po audycie ochrony danych osobowych ze względu na zmianę uwarunkowań zewnętrznych, jak i wewnętrznych powinna być ona aktualizowana.

22. SZKOLENIA UŻYTKOWNIKÓW

1) Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.

2) Za przeprowadzenie szkolenia odpowiada IOD lub wyznaczony przez niego zastępca, a za jego zorganizowanie odpowiada przełożony użytkowników.

3) Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami RODO oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.

4) Szkolenie zostaje zakończone podpisaniem listy obecności na szkoleniu.

23. PROCEDURA ZABEZPIECZENIA SYSTEMU INFORMATYCZNEGO, W TYM PRZED WIRUSAMI KOMPUTEROWYMI

1) Ochrona antywirusowa

a) Celem procedury jest zabezpieczenie systemów informatycznych przed szkodliwym oprogramowaniem (np. typu robaki, wirusy, konie trojańskie, rootkity) oraz nieautoryzowanym dostępem do systemów przetwarzających dane osobowe.

b) Za zaplanowanie i zapewnienie ochrony antywirusowej odpowiada ADO, w tym za zapewnienie odpowiedniej ilości licencji dla użytkowników.

c) System antywirusowy zainstalowano na wszystkich stacjach roboczych.

d) System antywirusowy zapewnia ochronę: systemu operacyjnego, przechowywanych plików, poczty wychodzącej i przychodzącej.

e) System operacyjny oraz pliki skanowane są programem antywirusowym w sposób automatyczny.

f) ADO zapewnia stałą aktywność programu antywirusowego tzn. program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe.

g) Aktualizacja definicji wirusów odbywa się automatycznie przez system.

h) W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić ADO.

2) Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

a) Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów.

b) Za zaplanowanie, konfigurowanie, aktywowanie specjalistycznego oprogramowania monitorującego wymianę danych na styku sieci lokalnej odpowiada ADO.

c) Stosowany jest Firewall.

d) Sieć bezprzewodową zabezpieczono hasłem.

e) Zastosowano mechanizmy monitorujące przeglądanie Internetu przez użytkowników. Uwzględniają one:

   i. Blokowanie stron internetowych określonego typu;

   ii. Blokowanie określonych stron internetowych;

   iii. Analizę przesyłanych informacji pod kątem niebezpiecznego oprogramowania.

24. PROCEDURA WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI

1) Procedura wykonywania przeglądów i konserwacji

Celem procedury jest zapewnienie ciągłości działania systemów informatycznych przetwarzających dane osobowe oraz zabezpieczenie danych osobowych przed ich nieuprawnionym udostępnieniem.

2) Przeglądy i konserwacje systemu informatycznego i aplikacji

a) ADO odpowiada za bezawaryjną pracę systemu IT, w tym: stacji roboczych, aplikacji serwerowych, baz danych, poczty email.

b) Przegląd i konserwacja systemu informatycznego powinny być wykonywane w terminach określonych przez producentów systemu lub zgodnie z harmonogramem ADO, jednak nie rzadziej, niż raz w roku.

c) Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ADO. ADO może wyznaczyć w tym celu wykonawcę.

d) ADO odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków.

e) ADO odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, drukarek, baz danych, poczty e-mail.

f) ADO odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.

g) Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego, wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.

h) Czynności konserwacyjne i naprawcze wykonywane doraźnie przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych), muszą być wykonywane pod nadzorem osób upoważnionych.

i) Przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza teren organizacji, należy:

i. wymontować nośniki z danymi osobowymi,

ii. trwale usunąć dane osobowe z użyciem specjalistycznego oprogramowania,

iii. nadzorować proces naprawy przez osobę upoważnioną przez administratora systemu, gdy nie ma możliwości usunięcia danych z nośnika.

3) Aktualizacje oprogramowania

a) ADO odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji.

b) ADO odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.

25. PROCEDURA NADAWANIA UPRAWNIEŃ I POSTĘPOWANIA Z DANYMI W ZAKRESIE KART PŁATNICZYCH

1) Spółka zobowiązuje się do poszanowania prywatności wszystkich swoich klientów oraz do ochrony wszelkich danych w zakresie kart płatniczych przed podmiotami zewnętrznymi.

2) Spółka nie przetwarza danych osobowych właścicieli kart płatniczych. Jedyną dostępną dla Spółki informacją są cztery ostatnie numery karty płatniczej.

3) W uzasadnionych przypadkach, Spółka może uzyskać pełny numer karty płatniczej, ubiegając się o to u dostawcy terminala płatniczego.

4) Ujawnienie pełnego numeru karty płatniczej odbywa się po uprzedniej weryfikacji przez dostawcę terminala płatniczego.

5) Prezes Spółki może upoważnić swojego pracownika do uzyskania w jego imieniu, w uzasadnionym przypadku, pełnego numeru karty płatniczej od dostawcy terminala.

6) Wszystkie upoważnione osoby, które otrzymają dostęp do poufnych danych tj. pełnego numeru karty płatniczej powinni zapewnić następujące środki bezpieczeństwa:

a) przetwarzać informacje o numerach kart w sposób zapewniający poufność;

b) ograniczyć korzystanie z systemów informatycznych i telekomunikacyjnych do wymiany informacji na temat numerów kart płatniczych;

c) nie ujawniać numerów kart płatniczych nieupoważnionym osobom;

d) przechowywać numery kart płatniczych w sposób uniemożliwiający dostęp osobom postronnym;

e) zawsze pozostawiać miejsce pracy bez poufnych danych;

f) incydenty związane z bezpieczeństwem danych w postaci numerów kart płatniczych zgłaszać bezzwłocznie osobie odpowiedzialnej za lokalne reagowanie na zdarzenia.

7) Wszystkie poufne dane właścicieli kart przechowywane i przetwarzane przez Spółkę i jej pracowników muszą być przez cały czas skutecznie zabezpieczone przed nieupoważnionym wykorzystaniem.

8) Wszystkie dane dot. kart płatniczych należy bezpiecznie usunąć, gdy nie będą już potrzebne Spółce, niezależnie od rodzaju nośników lub aplikacji, w których są przechowywane.

26. REGULAMIN UŻYTKOWANIA KOMPUTERÓW PRZENOŚNYCH

1) W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Pracodawcy, Użytkownik zobowiązany jest do ich przechowywania ich na dysku szyfrowanym (np. BitLocker) lub urządzeniu szyfrowanym w przypadku, gdy urządzenie to wynoszone jest poza firmę.

2) W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik ma obowiązek natychmiast powiadomić o tym Administratora/IOD lub bezpośredniego przełożonego, zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.

3) Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu.

4) W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp.

5) W przypadku pozostawiania komputerów przenośnych w biurze należy umieszczać je po zakończeniu pracy w zamykanych szafkach (zapisu nie stosuje się wobec administratorów sieci oraz innych osób, których charakter pracy nie pozwala na zastosowanie zapisu).

6) Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

27. REJESTR CZYNNOŚCI PRZETWARZANIA

Nazwa i dane kontaktowe Administratora:
Dane kontaktowe Inspektora Ochrony Danych:

Nazwa dokumentu – czynności przetwarzania	Osoba, która ma dostęp do dokumentu wewnątrz jednostki	Opis celu przetwarzania	Kategorie osób, których dane dot	Kategorie danych osobowych	Podstawa prawna	Źródło danych	Czas przetwarzania	Współadministrator	Transfer do kraju trzeciego	Nazwa podmiotu przetwarzającego	Kto przetwarza na zewnątrz	Nazwa systemu lub oprogramowania	Opis środków technicznych i organizacyjnych	Nazwa zbioru danych
			yczą											

28.REJESTR KATEGORII CZYNNOŚCI PRZETWARZANIA

Nazwa i dane kontaktowe Administratora:							
Dane kontaktowe Inspektora Ochrony Danych:							
Kategorie przetwarzania	Opis środków technicznych i organizacyjnych	Dane administratora	Dane IOD Administratora	Dane współadministratora	Czas trwania przetwarzania	Transfer do kraju trzeciego	Dokumentacja

radca prawny
Anna Mianowska
KT 2708